情報セキュリティポリシー

第一章　目的及び適用対象

（目的）

第一条 一般財団法人国土技術研究センター（以下「当財団」という）において、業務を継続的且つ安定的に実施し、社会的信用を維持していくためには、適切な情報セキュリティ対策を実施することが必要不可欠である。このため、内閣官房情報セキュリティセンターが情報セキュリティ政策会議において定めた政府機関の情報セキュリティ対策のための統一規範（以下「統一規範」という。）を参照し、当財団の特性を勘案し、情報セキュリティを確保するため、情報セキュリティポリシーを策定する。

（適用対象）

第二条 情報セキュリティポリシーの適用対象とする機関は当財団とする。

２ 情報セキュリティポリシーの適用対象とする者は、当財団役職員及び外部関係者とする。

３ 情報セキュリティポリシーの適用対象とする情報は、以下とする。

一　当財団役職員が職務上取り扱う情報であって、情報処理若しくは通信の用に供するシステム（以下「情報システム」という。）又は外部電磁的記録媒体に記録された情報又は紙媒体による情報

二　情報システムの設計又は運用管理に関する情報であって、情報処理若しくは情報システム又は外部電磁的記録媒体に記録された情報又は紙媒体による情報

第二章　情報セキュリティ対策のための基本方針

（情報セキュリティ文書）

第三条 当財団は、情報セキュリティポリシー及び、情報セキュリティ対策標準（以下「対策標準」という。）を定める。

２ 情報セキュリティポリシーは、情報セキュリティを確保するため、情報セキュリティ対策の目的、対象範囲等の情報セキュリティに対する基本的な考え方を定める。

３ 対策標準は、前項に定めた基本的考え方に基づいた情報セキュリティ対策が可能となるように、情報セキュリティ対策の基準を定める。

４ 当財団は、第十一条第一項の評価結果を踏まえ、情報セキュリティポリシーの評価及び見直しを行う。

第三章　情報セキュリティ対策のための基本対策

（管理体制）

第四条 当財団は、情報セキュリティ対策を実施するための組織・体制を整備する。

２ 当財団は、最高情報セキュリティ責任者１人を置く。

３ 最高情報セキュリティ責任者は、情報セキュリティポリシー等の審議を行う機能を持つ組織として情報セキュリティ委員会を設置し、委員長及び委員を置く。

４ 最高情報セキュリティ責任者は、情報セキュリティポリシーにて規定した情報セキュリティ対策に関する事務を統括するとともに、その責任を負う。

５ 最高情報セキュリティ責任者は、対策標準に定められた自らの担務を、対策標準に定める責任者等に担わせることができる。

（対策推進計画）

第五条 最高情報セキュリティ責任者は、第十一条第一項の評価の結果を踏まえた情報セキュリティ対策を総合的に推進するための計画（以下「対策推進計画」という。）を定める。

２ 当財団は、対策推進計画に基づき情報セキュリティ対策を実施する。

３ 最高情報セキュリティ責任者は、前項の実施状況を評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、対策推進計画の見直しを行う。

（例外措置）

第六条 当財団は、情報セキュリティポリシーに定めた情報セキュリティ対策の実施に当たり、例外措置を適用するために必要な申請・審査・承認のための手順と担当者を定める。

（教育）

第七条 当財団は、当財団役職員が自覚をもって情報セキュリティポリシーに定められた情報セキュリティ対策を実施するよう、情報セキュリティに関する教育を行う。

（情報セキュリティインシデントへの対応）

第八条 当財団は、情報セキュリティインシデント（JIS Q 27000:2014 における情報セキュリティインシデントをいう。以下同じ。）に対処するため、適正な体制を構築するとともに、必要な措置を定め、実施する。

２ 情報セキュリティインシデントの可能性を認知した者は、対策標準に定める報告窓口に報告する。

３ 対策標準に定める統括情報セキュリティ責任者は、情報セキュリティインシデントに関して報告を受け又は認知したときは、必要な措置を講じる。

（自己点検）
第九条 当財団は、情報セキュリティ対策の自己点検を行う。

（監査）
第十条 当財団は、情報セキュリティ対策の内部監査を行う。

（リスク評価と対策）
第十一条 当財団は、第九条に定める自己点検の結果及び第十条に定める内部監査の結果等を踏まえ、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び顕在時の損失等を分析し、リスクを評価し、必要となる情報セキュリティ対策を講じる
２ 当財団は、前項の評価に変化が生じた場合には、情報セキュリティ対策を見直す。

（情報の格付）
第十二条 当財団は、取り扱う情報に、機密性、完全性及び可用性の観点に区別して、分類した格付を付す。
２ 当財団は、業務を実施するために必要となる情報の提供、運搬及び送信に際しては、前項で定めた情報の格付のうち、いかなる区分に相当するか明示等をする。

（情報の取扱制限）
第十三条 当財団は、情報の格付に応じた取扱制限を定める。
２ 当財団は、取り扱う情報に、前項で定めた取扱制限を付す。
３ 当財団は、業務を実施するために必要となる情報の提供、運搬及び送信に際しては、情報の取扱制限の明示等をする。

（情報のライフサイクル管理）
第十四条 当財団は、情報の作成、入手、利用、保存、提供、運搬、送信及び消去の各段階で、情報の格付及び取扱制限に従って必要とされる取り扱いが損なわれることがないように、必要な措置を定め、実施する。

（情報を取り扱う区域）
第十五条 当財団は、当財団が管理する施設又は当財団以外の組織から借用している施設等、当財団の管理下にあり、施設及び環境に係る対策が必要な区域の範囲を定め、その特性に応じて対策を決定し、実施する。

（外部委託）

第十六条 当財団は、情報処理に係る業務を外部委託する場合には、必要な措置を定め、実施する。

２ 当財団は、外部委託（約款による外部サービスの利用を除く。）を実施する場合は、委託先において情報漏洩対策や、委託内容に意図しない変更が加えられない管理を行うこと等の必要な情報セキュリティ対策が実施されることを選定条件とし、仕様内容にも含める。

３ 当財団は、要機密情報を約款による外部サービスを利用して取り扱ってはならない。

４ 当財団は、対策標準に定める基準に従い、機器等の調達を行う。

（情報システムに係る文書及び台帳整備）

第十七条 当財団は、所管する情報システムに係る文書及び台帳を整備する。

（情報システムのライフサイクル全般にわたる情報セキュリティの確保）

第十八条 当財団は、所管する情報システムの企画、調達・構築、運用・保守、更改・廃棄及び見直しの各段階において情報セキュリティを確保するための措置を定め、実施する。

（暗号・電子署名）

第十九条 当財団は、当財団における暗号及び電子署名の利用について、必要な措置を定め、実施する。

（インターネット等を用いた情報の提供）

第二十条 当財団は、ホームページ等を用いて情報を提供する際には、利用者端末の情報セキュリティ水準の低下を招く行為を防止するために、必要な措置を定め、実施する。

（情報システムの利用）

第二十一条 当財団は、情報システムの利用に際して、情報セキュリティを確保するために当財団役職員が行わなければならない必要な措置を定め、実施させる。

（対策標準への委任）

第二十二条 情報セキュリティポリシーに定めるもののほか、情報セキュリティポリシーの実施のための手続その他その執行について必要な細則は、対策標準で定める。

附則

この規程は、2018 年 4 月 10 日から施行する。